Critical Infrastructure Protection in the Communications Sector: Core Concepts

Anthony Critelli, B.S. ANSA 2014 & Dr. Sumita Mishra
aac3771@rit.edu sumita.mishra@rit.edu

Problem Description

The National Infrastructure Protection Plan (NIPP) and Communications Sector Specific Plan (SSP) developed by the Department of Homeland Security describe a clear framework for assessing, understanding, and mitigating risk in the Communications Sector. Although students in networking and communications courses gain the skills necessary to operate complex infrastructures, they often lack an understanding of critical infrastructure concepts.

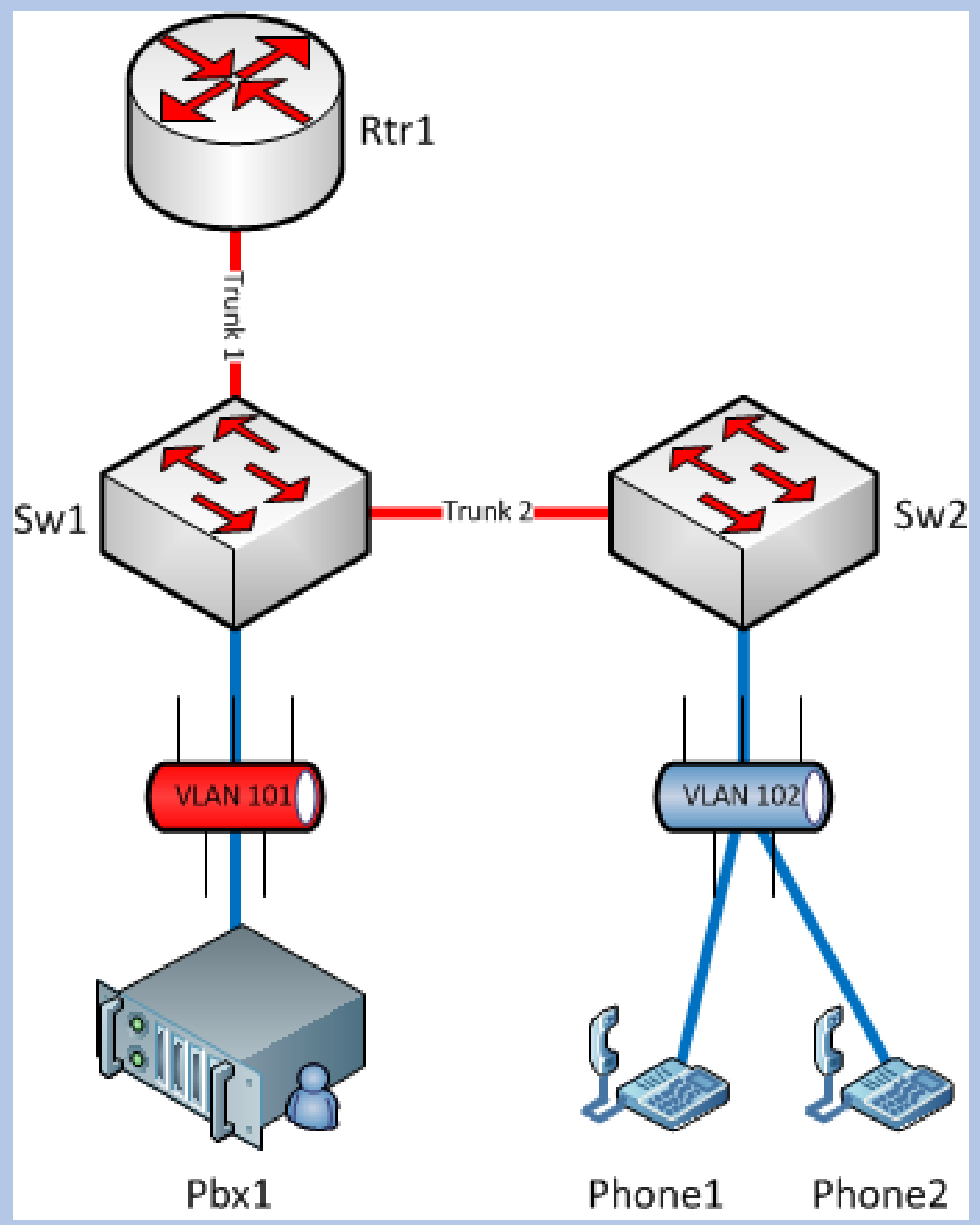
Solution

By developing a lab-based approach to CIP education, we are able to integrate infrastructure protection methods with existing learning opportunities for students. Our solution involves a modular approach that allows students to build small versions of real network topologies and then evaluate these infrastructures based on the NIPP and Communications SSP frameworks.

Lab Components

Lab Activities

Each student lab group constructs a topology based on a set of network requirements. Lab activities and questions guide students to find vulnerabilities in their network design. A class internetwork provides a larger infrastructure for evaluation.

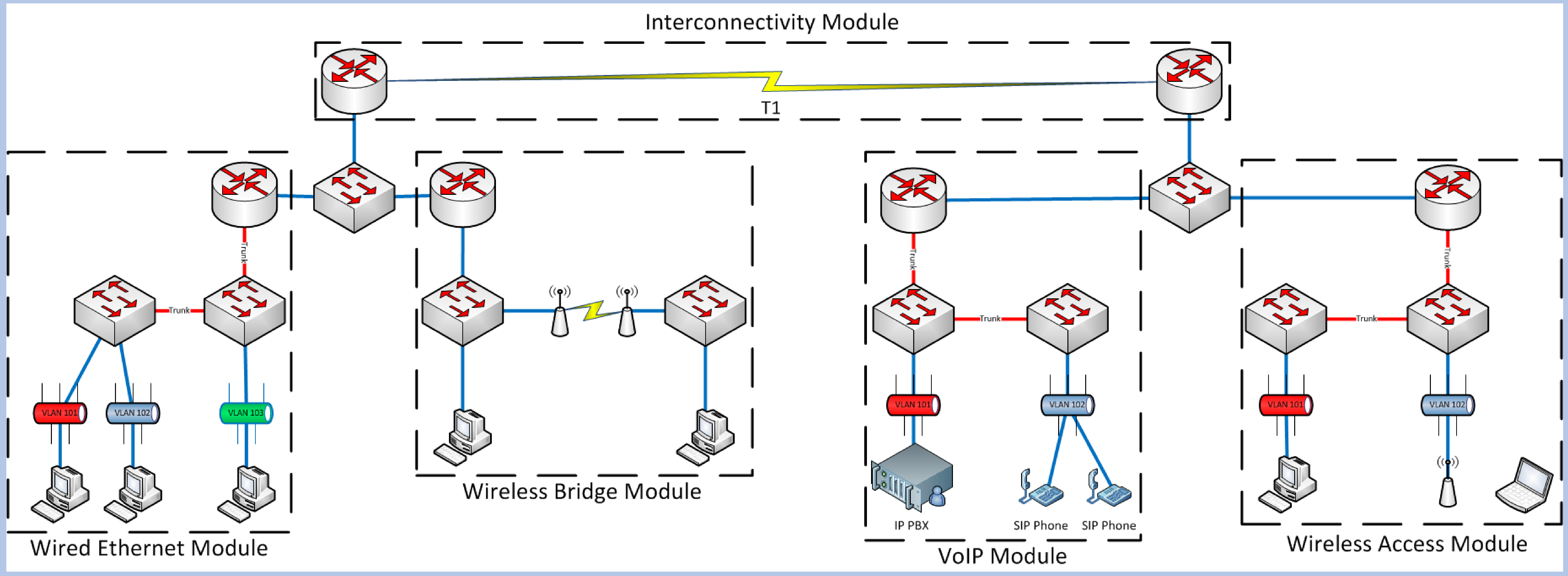


Lab Report

Each student submits a comprehensive lab report that follows the NIPP and Communications SSP framework. General framework questions, combined with topology-specific questions, provide guidance for risk assessment and planning.

CIP Concepts

Through lab exercises, students explore the critical infrastructure protection process. Students will set goals, identify assets, assess risks, prioritize infrastructure, develop protection strategies, and review the effectiveness of their strategies.


Interconnectivity Module
T1
Trunk
VLAN 101
VLAN 102
VLAN 103
Wired Ethernet Module
Wireless Bridge Module
IP PBX
SIP Phone
SIP Phone
VoIP Module
Wireless Access Module